Introduction (Section:2m, Total:2m)

A. (Myself, nickname, call sign)

B. (Anecdote how presenter forcefully open sourced closed hardware)

C. (Some renowned software presenter made for conventions)

D. Amateur radio operator and 'stuff hacker'

Basics of SigInt (Section:8m, Total:10m)

A. What is it?

1. Signals intelligence (SIGINT) is intelligence-gathering by interception of signals, whether communications between people (communications intelligence—abbreviated to COMINT) or from electronic signals not directly used in communication (electronic intelligence—abbreviated to ELINT). -- Wikipedia

B. Why do we care?

1. Unknown - Lots of things use radio. Equipment to read used to be $$$$ and relied on obscurity. Not now.

2. Unencrypted - Just like IoT, the E stands for Encryption. Most encryption is "we use diff. frequencies"

3. Unauthenticated \

4. Unauthorized |-- AAA Stack. Authentication, Authorization, Auditing. We'll have none of that.

5. Unauditable /

6. HACKED - Various holes enable taking control of endpoints, or listening in on sensitive data

SigInt Platforms (Section:16m , Total:26m)

A. Demo Platform

1. Raspberry Pi 3(All but PiB works)

a. I used RasPi 3 B+

2. Touchscreen that uses DSI or HDMI. Absolutely cannot use GPIO4

a. I used 7 in HDMI with usb power/touchscreen interface

3. RTLSDR dongle

a. I bought the el cheapo $8 Ali express special. Many will work. Make sure to get a TXCO (temp controlled oscillator) enabled

4. Good battery that outputs 2.5A or better USB

5. Antennas

a. omni

b. yagi

c. "weird" antennas

d. freq restrictions of hardware

i. RPi is 10KHz-1.5GHz TX

ii. RTLSDR is 24MHz-1.7GHz RX

iii. Ideal to find 2 antennas good from 24MHz-1.5GHz for symmetric bidirectional comms

6. Odds and ends

a. SMA and RP SMA connectors

b. Kapton tape for insulation

c. Lots and lots of time!

B. Other hardware you can use

1. Transmit & Receive

a. ADALM-PLUTO - 70MHz-6GHz full duplex. 5mw (DINKY) but is only $100 !

b. HackRF One - 1 MHz to 6 GHz single duplex. Tx OR Rx at any given time. ~$300

c. USRP SDRs - set top boxes, USB3 and/or ethernet. $$$$$$$$$

2. Receive only

a. Lots of RTLSDR usb devices. Prices range from $6 to $50. Many form factors. All use the Realtek R820T2 chip

a. KerberosSDR - Coherent "Quad Damage RTLSDR". Shipping Mid-late Jan 2019. Can do triangulation and signal tracking realtime.

b. NooElec NESDR SMArTee XTR - $40 for 65MHz-2300MHz

Software Stacks and Tools (Section:20m, Total:46m)

A. Review of the Fun Tools

1. Linux (Raspbian)

2. RPITX - Library that turns a dumb RPi into a full transmitter from 10KHz-1.5GHz . Also allows TX using raw IQ!

3. rtl\_\* commands - RTLSDR libraries and commands to natively interact with the RTLSDR. Other programs also rely on them incl RPITX

4. GnuRadio - Best way to build a targeted attack platform for a specific encoding and interaction. Steep curve to learn. Lots of modules.

a. gr-inspector is a ML module to find "Yummies" in signals. Think of this as a radio anomaly detector, so we don't have to look ourselves.

5. GQRX - Really QT frontend for Gnuradio to 'surf the waves' and see what's going on through a swath of spectrum

6. Salamandra - a tool to dynamically find spy microphones. Uses SDR closed loop to catch red handed. Detects AND locates.

7. TempestSDR - SDR tool that receives and decodes RF interference from monitors and shows what they display

(Note to reviewers: SigInt is 'The Next Big Thing', and has a great deal of focus on it right now. This section may expand as new tools are made by myself or the community in the coming months up to the talk. Other sections that will be reduced in time will be 'Other hardware you can use', followed by 'Demo Platform', as the knowledge to DIY it will be more widespread.)

Demonstration (Section:6m, Total:52m)

A. Record/Playback of audio over amateur radio frequency using Demo Platform and Baofeng

B. Replay attack demonstrated of a common 433MHz "arduino" module for IoT setups

Q&A (Section:8m, Total:60m)

Citations (shown on screen, not spoken):

A. RPi

B. RPITX

C. Gnu/Linux

D. Raspbian

E. GnuRadio

F. GQRX

G. Salamandra

H. TempestSDR

Acknowledgements (shown on screen, not spoken):

A. WarCollar industries, for getting me to think in this direction (and awesome story)